Manuel d'installation et d'utilisation de Tkontrole 2.0

Tkontrole version 2.0

Contenu de cette documentation

Présentation et installation....4

Licence de cette documentation....5

Pourquoi Tkontrole ?....5

Existence et correction des bugs....5

Architecture du logiciel - terminologie....6

Plateformes supportées....6

Installation sous Windows....6
Partie serveur....6
Partie client....8

Installation sous Linux....8
Partie serveur....8
Partie client....9

Configuration....9
Partie serveur....9
Partie client....10
Écriture des adresses des machines....12

La sécurité face aux éventuels pirates....14
Contrôle des adresses ou des noms....14
Mot de passe de connexion....14

Désinstallation sous Windows....15
Partie serveur....15
Partie client....15

Désinstallation sous Linux....15
Partie serveur....15
Partie client....16

Mode d'emploi de Tkontrole-client....17

Aspect général....18

Démarrage....18

Affichage des ordinateurs placés sous contrôle....18

Agir sur les ordinateurs....19
Agir sur un seul ordinateur....20
Agir sur un ensemble d'ordinateurs....20

Les différentes actions disponibles....21
Action « Rafraichir »....21
Action « Voir en taille réelle »....21
Action « Voir les écrans »....21
Action « Enregistrer les écrans »....21

Action « Prendre le contrôle »....21
Action « Faire une démo »....21
Action « Bloquer les machines »....22
Action « Bloquer lnternet »....22

Comportement quand le client est arrêté....22

Comportement quand le serveur est redémarré....22
Action « Ecrire »....23
Action « Eteindre »....23

Revoir une séquence enregistrée....24

Annexes....25

Architecture du logiciel....26

Format du fichier Tkontrole-serveur.cfg....27
Utilité....27
Syntaxe du fichier....27
Exemple....27

Format du fichier tkontrole-client.cfg....30
Utilité....30
Syntaxe....30
Exemple....30

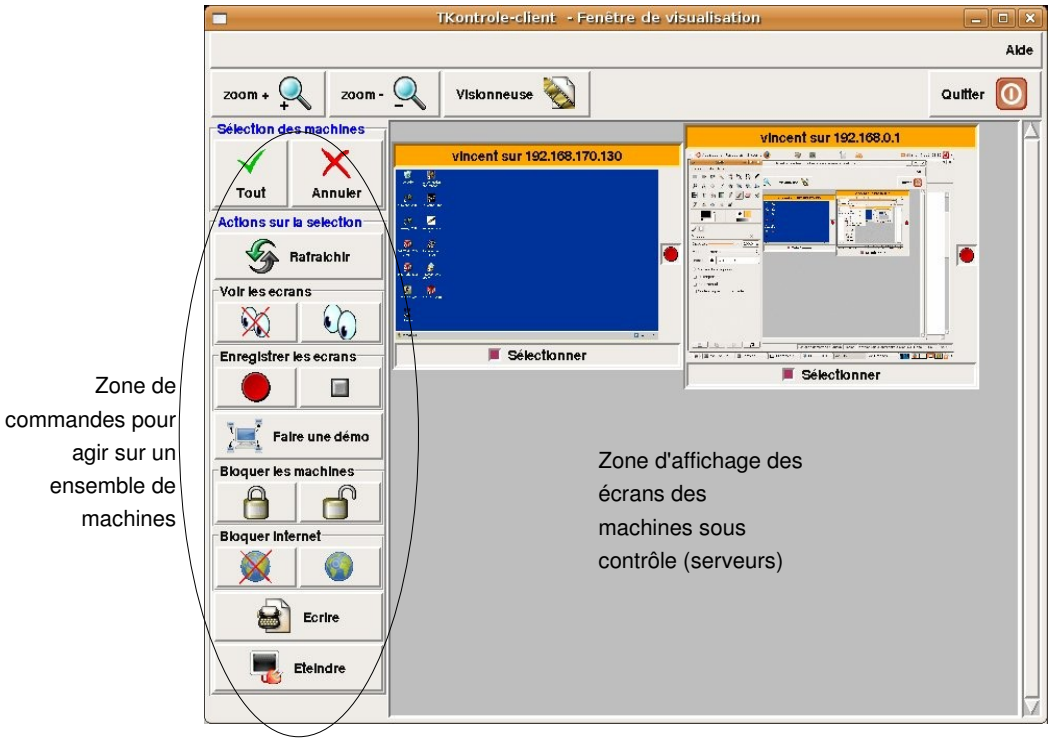
Protocole utilisé par Tkontrole....32
Version du protocole décrite : 1.1....32
Description du protocole de connexion au serveur....32

Mode d'emploi de Tkontrole-client

Aspect général

Quand Tkontrole-client est démarré, une fenêtre s'ouvre

Cette fenêtre comporte un ensemble de boutons et une zone d'affichage des ordinateurs sous contrôle.



Démarrage

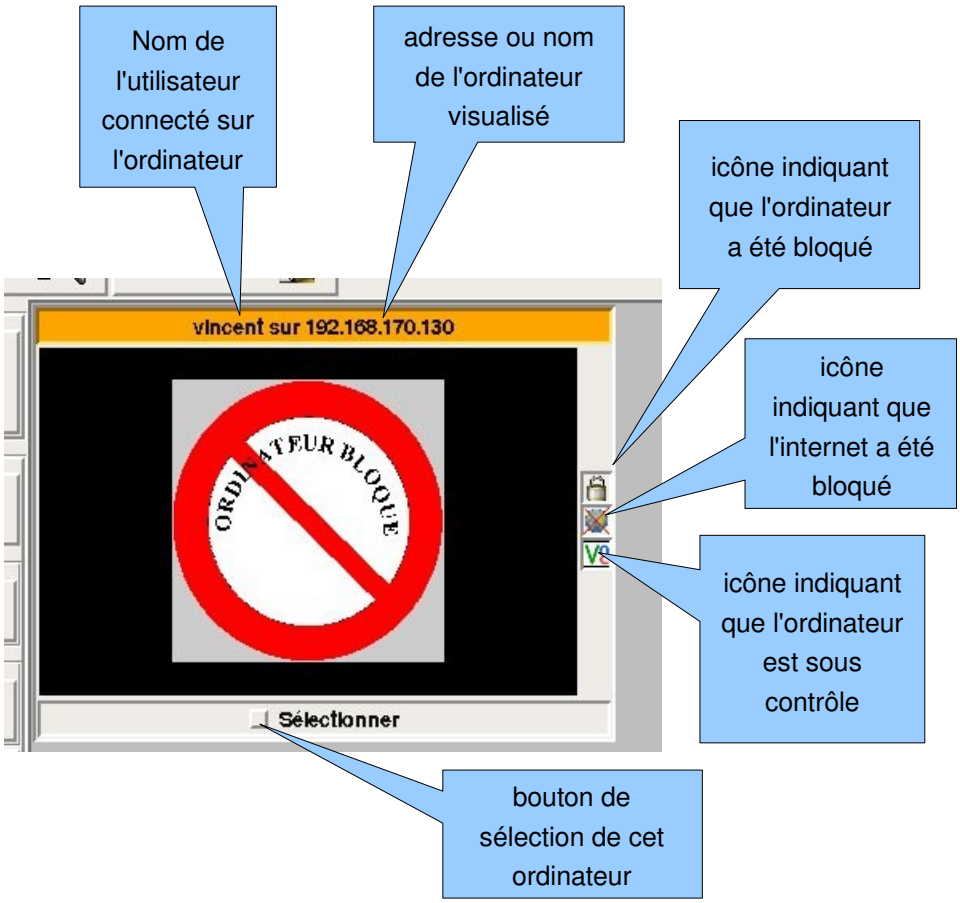
En phase de démarrage, la zone d'affichage des écrans montre une barre de progression qui indique que le client recherche les postes serveurs à surveiller. Tant qu'aucune machine n'est trouvée ou accepte la connexion, la barre continue à s'afficher.

Affichage des ordinateurs placés sous contrôle

Dès qu'un ordinateur sous contrôle est démarré, une nouvelle fenêtre de visualisation apparaît dans la zone d'affichage des écrans. Selon les cas, on voit une capture de l'écran ou alors une icône indiquant que la capture d'écran est désactivée.

La capture d'écran est désactivée	La capture d'écran est activée

La fenêtre de visualisation apporte de nombreuse informations :


Nom de l'utilisateur connecté sur l'ordinateur
adresse ou nom de l'ordinateur visualisé
icône indiquant que l'ordinateur a été bloqué
icône indiquant que l'internet a été bloqué
icône indiquant que l'ordinateur est sous contrôle
bouton de sélection de cet ordinateur
vincent sur 192.168.170.130
Sélectionner

Agir sur les ordinateurs

Tkontrole permet d'agir soit sur un ordinateur seul, soit sur un ensemble d'ordinateurs sélectionnés.

Agir sur un seul ordinateur

Il suffit de cliquer sur la fenêtre de visualisation (clic gauche ou droit). Une boite à boutons contextuelle apparaît :

Agir sur un ensemble d'ordinateurs

Il faut pour cela sélectionner les ordinateurs.

Si l'on souhaite agir sur l'ensemble des ordinateurs démarrés, il suffit de cliquer sur le bouton « Tout » disponible sur la gauche de la fenêtre de Tkontrole-client.

Bien entendu, si l'on appuie sur « Annuler », on annule toute sélection déjà effectuée.

Il est aussi possible de sélectionner des ordinateurs un à un. Il suffit pour cela de cliquer sur la case à cocher en dessous de la fenêtre de visualisation de l'ordinateur.

Il suffit ensuite de choisir le bouton correspondant à l'action désirée pour qu'elle soit appliquée à l'ensemble des ordinateurs sélectionnés.

Les différentes actions disponibles

Action « Rafraichir »

Provoque l'affichage d'une nouvelle capture d'écran sur le (ou les) écran sélectionné.

Action « Voir en taille réelle »

Provoque l'affichage en taille réelle de l'écran de l'ordinateur concerné.

Action « Voir les écrans »

Provoque l'affichage de l'écran de l'ordinateur sélectionné.

Action « Enregistrer les écrans »

Démarre l'enregistrement de toutes les captures d'écran sur le (ou les) ordinateur sélectionné. On peut ensuite revoir l'enregistrement grâce à la visionneuse (voir plus loin).

Remarques :

L'enregistrement est constitué de la suite des captures d'écrans. Ces captures sont des images au format gif.
La taille d'une capture est de l'ordre de 50 ko. A raison d'une capture toutes les 10 s, un enregistrement d'une heure a une taille approximative inférieure à 20 Mo, donc très peu !

Les enregistrement sont enregistrés dans le dossier spécifié ors de la configuration. Dans ce dossier est créé automatiquement un dossier tkontrole. Dans ce sous-dossier est créé un sous dossier à la connexion d'un utilisateur. Ce sous-dossier est nommé : nom_de_l'utilisateur-nom_de _machine.

Action « Prendre le contrôle »

Cela permet de prendre le contrôle sur la machine considérée.

Remarque : Tkontrole-serveur, quand il reçoit cet ordre de la part du client, démarre un serveur VNC dédié à cette prise de contrôle. Le serveur est automatiquement arrêté quand le contrôle prend fin.

Action « Faire une démo »

Cette fonctionnalité permet d'envoyer une démonstration à (aux) l'ordinateur sélectionné. C'est à dire que l'ordinateur sélectionné voit tout ce qui se passe sur l'écran du poste de contrôle (Tkontrole-client).

Pour mettre fin à la démo, il suffit d'appuyer sur le bouton

.

Remarque : Tkontrole-client démarre un serveur VNC pour faire cela. Le serveur est coupé automatiquement à l'arrêt de la démo.

Action « Bloquer les machines »

Provoque l'apparition d'une image sur l'écran (par défaut un panneau « ordinateur bloqué »).

L'utilisateur ne peut plus utiliser son ordinateur jusqu'au déblocage.

Action « Bloquer Internet »

Provoque le blocage de l'internet.

L'utilisateur ne peut plus naviguer sur la toile jusqu'au déblocage.

Comportement quand le client est arrêté

Les postes placés sous contrôle (les serveurs) qui étaient bloqués sont automatiquement débloqués.

Par contre, le blocage de l'internet reste tel qu'il était, tant que l'ordinateur n'est pas redémarré.

Comportement quand le serveur est redémarré

C'est le cas par exemple quand on a bloqué un poste et que l'utilisateur de cet ordinateur décide de redémarrer l'ordinateur, pensant échapper au blocage.

Tant que le poste de contrôle reste actif, c'est à dire que le client fonctionne, il y a mémorisation de l'état de chaque poste placé sous contrôle. ainsi, quand l'ordinateur de l'utilisateur sera redémarré, il se retrouvera à nouveau sous contrôle du client qui imposera automatiquement à nouveau le blocage ! Il en est de même pour les autres actions, telles que l'enregistrement, la prise de contrôle ou le blocage de l'internet.

Action « Ecrire »

Permet d'envoyer un message à la (ou les) machine sélectionnée.

Une fenêtre s'ouvre, permettant de saisir le message.

Une fois saisi, il suffit de cliquer sur le bouton « Envoyer ». Le destinataire reçoit le message, qui s'affiche dans une fenêtre semblable :

Il est informé du nom de l'auteur du message (bandeau orange).

Action « Eteindre »

Provoque l'arrêt, le redémarrage ou la déconnexion du (ou des) ordinateurs sélectionné(s). Une fenêtre permet au préalable de choisir l'action voulue.

remarque : l'utilisateur de la machine qui reçoit l'ordre de s'arrêter ou de se déconnecter n'a pas possibilité de contrôler l'arrêt. Donc, il faut bien faire attention à ce que son travail soit enregistré avant !

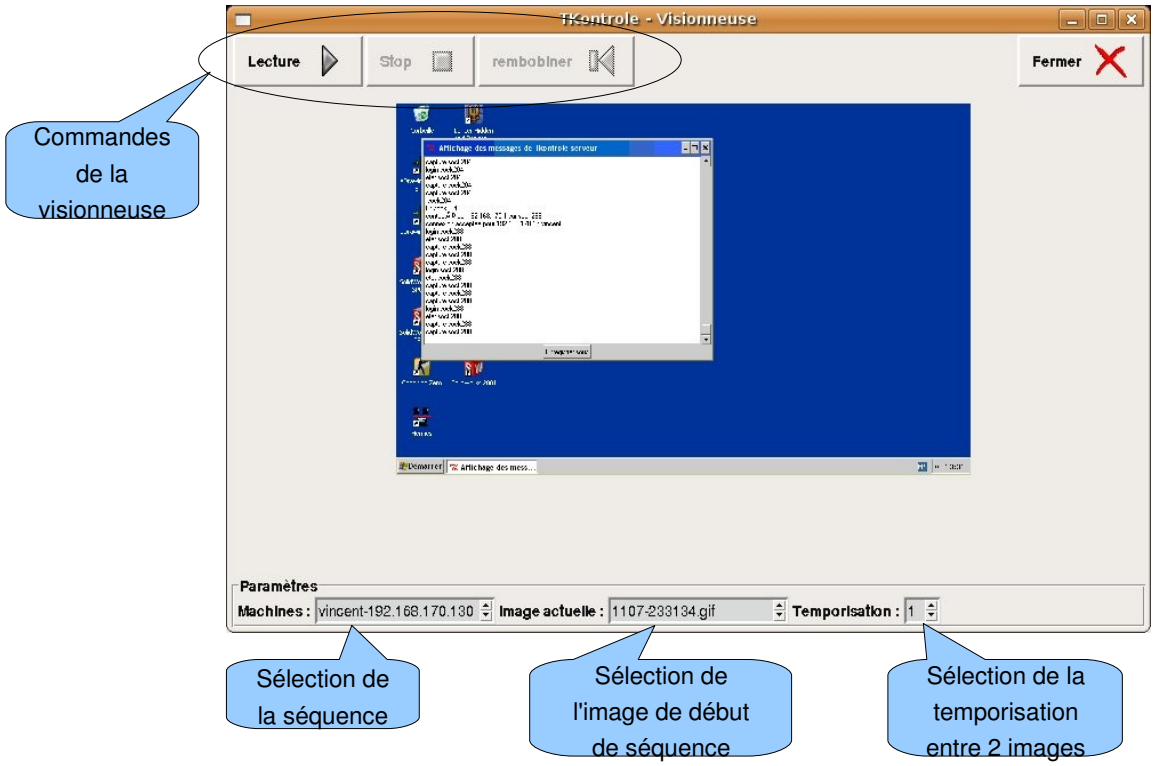
Revoir une séquence enregistrée

Des captures d'un ou plusieurs ordinateurs ont été enregistrées.

Pour les revoir, il suffit de faire apparaître la visionneuse en cliquant sur le bouton

.

L'illustration ci-dessous montre les différentes commandes et fonctions de cette visionneuse.



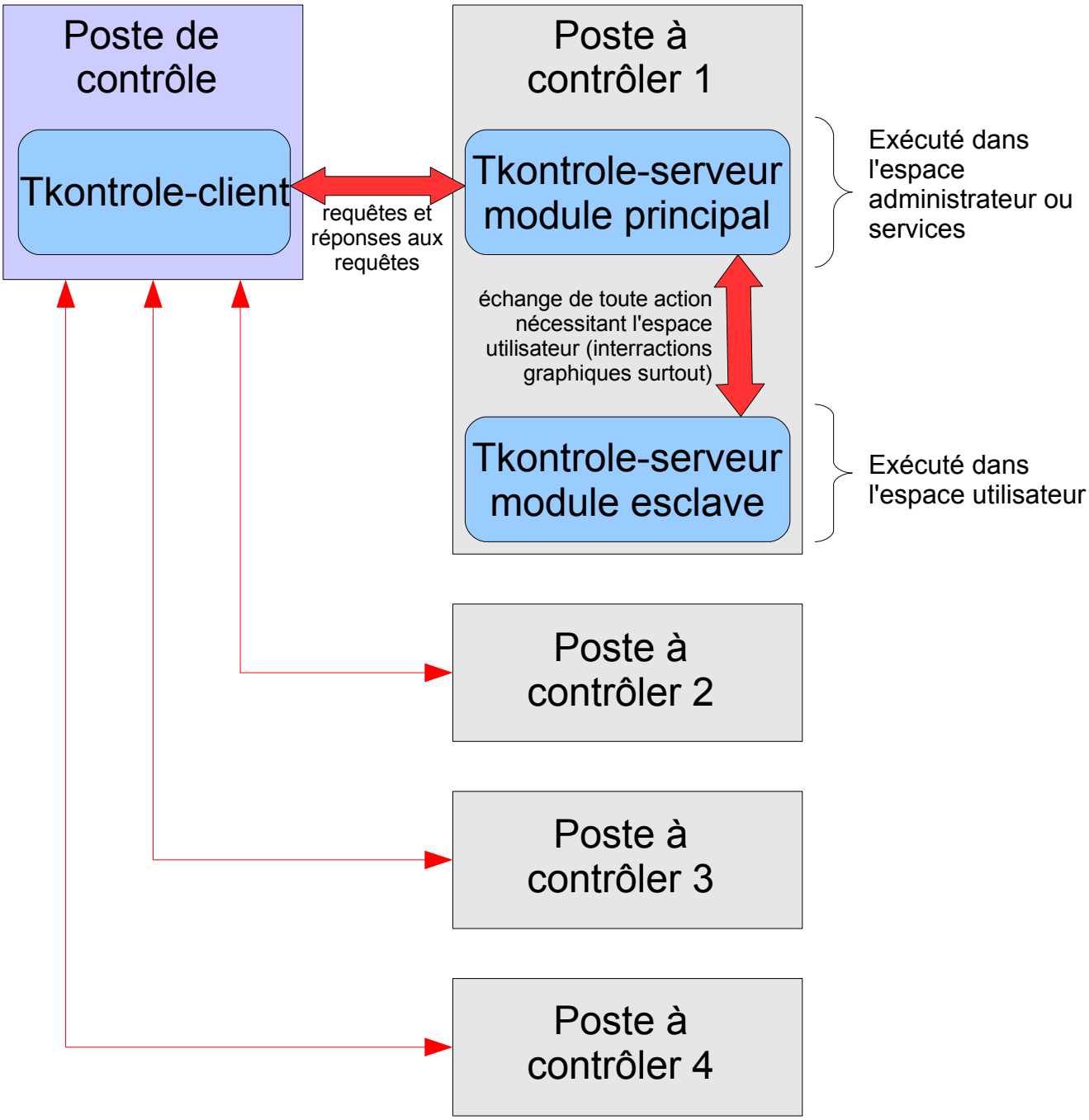
Il suffit de sélectionner la machine et l'utilisateur puis d'appuyer sur « lecture ».

Éventuellement, on peut se déplacer dans la séquence en sélectionnant une image dans la zone de sélection prévue.

Annexes

Architecture du logiciel

Le diagramme ci-dessous montre que le logiciel est composé d'un client et d'un serveur, techniquement décomposé en 2 modules : serveur et esclave du serveur. Cette architecture, nouvelle depuis la version 2.0 et imposée pour le portage sous Windoze Vista.


Poste de contrôle
Tkontrole-client
requêtes et réponses aux requêtes
Poste à contrôler 1
Tkontrole-serveur module principal
Exécuté dans l'espace administrateur ou services
échange de toute action nécessitant l'espace utilisateur (interractions graphiques surtout)
Tkontrole-serveur module esclave
Exécuté dans l'espace utilisateur
Poste à contrôler 2
Poste à contrôler 3
Poste à contrôler 4

Format du fichier Tkontrole-serveur.cfg

Utilité

Ce fichier permet de configurer le serveur Tkontrole.

Syntaxe du fichier

Les commentaires sont précédés du signe #.

Exemple

```
#########################################################################
#Programme écrit par V. Verdon
#TKontrole est un utilitaire de surveillance d'ordinateurs
#placé sous licence GNU GPL (consulter le fichier joint intitulé "licence.txt"
#########################################################################
# TKontrole version 2.0
# Fichier de configuration du serveur

# Adresse sur laquelle le serveur écoute
# Si la valeur est vide, alors la première interface réseau est utilisée
set ip_serv {192.168.0.1}

# Adresse du serveur d'administration de Tkontrole (maj notamment)
set ip_admin {}
#set ip_admin 192.168.0.1

# Adresses de clients acceptées
set ip_accept {127. 172. 192.168. 10.}
# set ip_accept {{$ip(a).$ip(b).$ip(c).199} pc1 192.168.0.1 {pc<10 15>}}
#set ip_accept {192.169.130.199}

# Port utilisé par Tkontrole
set port 4444

# Port utilisé par VNC depuis Tkontrole
set port_vnc 4445

# Affichage d'une info indiquant que le poste est surveillé
# valeurs possibles : 2 (affichage d'une boite d'info à la connexion), 1 (affichage d'un bandeau permanent) ou 0 (pas
d'affichage)
set info_surv 2

# Message affiché indiquant que le poste est surveillé
set message_surv "Cet ordinateur est placé sous surveillance"

# état de la route par défaut 1=bloquée (pas d'internet) , 0=débloquée
set blocage_route_init 0

# liste des ports a bloquer en mode blocage de l'internet (sans effet sous Win98-Me)
set firewall(liste_ports_bloques) {21t 21u 25t 80t 80u 110t 110u 443t 443u}

# Mettre ce paramètre à 1 pour avoir la console de débuggage
set debug 1
```

```
# Ne pas modifier en dessous de cette ligne ... sauf si vous savez ce que vous faites !
###############################################################################
###############################################################################

switch $::os {
  {nt} {
    # config Win NT2000 et XP
    set exe_arret {$::rep/bin/shutdown.exe -u -f}
    set exe_deconnexion {$::rep/bin/shutdown.exe -l -f}
    set exe_redemarrage {$::rep/bin/shutdown.exe -r -f}
    set exe_capture {$::rep/bin/capture_ecran_gif.exe $::rep_tmp/$::fic_capture}
    set exe_kill {$::rep/bin/kill.exe}
    set exe_vncviewer {$::rep/bin/vncviewer.exe $ip:$::port_vnc FullScreen=1}
    set exe_vncserver {$::rep/bin/winvnc4.exe SecurityTypes=None Hosts=+$ip/255.255.255.255 PortNumber=
$::port_vnc NeverShared=1 DisableClose=1 DisableOptions=1}
    set rep_tmp $env(temp)
  }

  {98} {
    # config Win 95 98 et Me
    set exe_arret {$::rep/bin/arreter.exe}
    set exe_capture {$::rep/bin/capture_ecran_gif.exe $::rep_tmp/$::fic_capture}
    set exe_kill {$::rep/bin/kill.exe}
    set exe_vncviewer {$::rep/bin/vncviewer.exe $ip:$::port_vnc FullScreen=1}
    set exe_vncserver {$::rep/bin/winvnc4.exe SecurityTypes=None Hosts=+$ip/255.255.255.255 PortNumber=
$::port_vnc NeverShared=1 DisableClose=1 DisableOptions=1}
    set rep_tmp $env(temp)
  }

  {linux} {
    # config Linux
    set exe_arret {/sbin/halt}
    set exe_deconnexion {$::rep/bin/deconnecter.sh}
    set exe_redemarrage {/sbin/reboot}
    set exe_capture {$::rep/bin/capture.sh $::rep_tmp/tmp  $::rep_tmp/$::fic_capture}
    set exe_kill kill
    # avec RealVnc, on écrit addr:port
    set exe_vncviewer {vncviewer $ip:$::port_vnc}
    # avec TightVnc, on écrit addr::port
    # set exe_vncviewer {vncviewer $ip::$::port_vnc}
    set exe_vncserver {x11vnc -display :0 -rfbport $::port_vnc -allow $ip}
    set rep_tmp /tmp
  }

  {vista} {
    # config Vista
    set exe_arret {$::rep/bin/shutdown.exe -u -f}
    set exe_deconnexion {$::rep/bin/shutdown.exe -l -f}
    set exe_redemarrage {$::rep/bin/shutdown.exe -r -f}
    set exe_capture {$::rep/bin/capture_ecran_gif.exe $::rep_tmp/$::fic_capture}
    set exe_kill {$::rep/bin/kill.exe}
    set exe_vncviewer {$::rep/bin/vncviewer.exe $ip:$::port_vnc FullScreen=1}
    set exe_vncserver {$::rep/bin/winvnc4.exe SecurityTypes=None Hosts=+$ip/255.255.255.255 PortNumber=
$::port_vnc NeverShared=1 DisableClose=1 DisableOptions=1}
    set rep_tmp $env(temp)
  }

  {inconnu} {
    # config autres Unix ?
```

```
    # config Linux
    set exe_arret {/sbin/halt}
    set exe_deconnexion {$::rep/bin/deconnecter.sh}
    set exe_redemarrage {/sbin/reboot}
    set exe_capture {$::rep/bin/capture.sh $::rep_tmp/tmp  $::rep_tmp/$::fic_capture}
    set exe_kill kill
    # avec RealVnc, on écrit addr:port
    set exe_vncviewer {vncviewer $ip:$::port_vnc}
    # avec TightVnc, on écrit addr::port
    # set exe_vncviewer {vncviewer $ip::$::port_vnc}
    set exe_vncserver {x11vnc -display :0 -rfbport $::port_vnc -allow $ip}
    # set exe_vncserver {x11vnc -display :0 -once -norc -bg -rfbport $::port_vnc -allow $::don($s,ip)}
    set rep_tmp /tmp
   }
}

 # Nom du fichier temporaire de capture
set fic_capture capture.gif

 # Nom du fichier temporaire de message
set fic_message message.txt
```

Format du fichier tkontrole-client.cfg

Utilité

Ce fichier permet de configurer le client Tkontrole.

Syntaxe

Les commentaires sont précédés du signe #.

Exemple

```
#########################################################################
#Programme écrit par V. Verdon
#TKontrole est un utilitaire de surveillance d'ordinateurs
#placé sous licence GNU GPL (consulter le fichier joint intitulé "licence.txt"
#########################################################################
# TKontrole version 2.0
# Fichier de configuration du client

# Port utilisé par Tkontrole
set port 4444

# Port utilisé par VNC depuis Tkontrole
set port_vnc 4445

# Mot de passe de connexion (si le fichier « pass » est inexistant côté serveur, aucun mot de passe exigé)
set password {essai}

# Répertoire personnel où seront stockées les données
# si on met  ~ : pointe automatiquement vers le dossier "mes documents"
# set rep_home h:/
set rep_home ~

# Liste des ordinateurs à surveiller
# set liste_ip {amphitheatre}
# set liste_ip {{b130p0<1 9>} {b130p<10 15>} }
# set liste_ip {{$ip(a).$ip(b).$ip(c).<1 15>}}
# set liste_ip {{b130p0<1 9>} {b130p<10 15>}}
set liste_ip {b130p100  192.169.130.198}

# La résolution de noms doit utiliser Netbios en plus de DNS (Unix/Linux uniquement)
set netbios 1

# ce paramètre définit si on fait la capture d'écran par défaut (1) ou non (0)
set etat_visu_defaut 1

# Délai entre 2 captures d'écran en seconde
set tempo(regen) 10

# Délai entre 2 recherches de serveurs TKontrole en seconde
set tempo(scan) 15

# valeur de réduction pour la visualisation des écrans (de 2 à 10)
set reduction 7
```

```
# Mettre ce paramètre à 1 pour avoir l'affichage des messages d'erreurs et autres
set debug 1


# Ne pas modifier en dessous de cette ligne ...
# sauf si vous savez exactement ce que vous faites !
################################################################################
################################################################################

# options concernant la recherche de serveurs dispo.
# Il peut être nécessaire d'augmenter cette valeur si le serveur ne répond pas (WinXP notamment)
# temps en milliseconde
set tempo(recherche) 100

switch $tcl_platform(os) {

   {Windows NT} {
      # config Win NT2000 et XP
      set exe_vncviewer {$::rep/bin/vncviewer.exe $::don($s,ip):$::port_vnc}
      set exe_demo {$::rep/bin/winvnc4.exe SecurityTypes=None Log=*:stdout:10 Hosts=$l_ip_m PortNumber=
$::port_vnc AlwaysShared=1 AcceptPointerEvents=0 AcceptKeyEvents=0 AcceptCutText=0}
      set exe_kill {$::rep/bin/kill.exe}
      set rep_tmp $env(temp)
   }

   {Windows 95} {
      # config Win 95 98 et Me
      set exe_vncviewer {$::rep/bin/vncviewer.exe $::don($s,ip):$::port_vnc}
      set exe_demo {$::rep/bin/winvnc4.exe SecurityTypes=None Log=*:stdout:10 Hosts=$l_ip_m PortNumber=
$::port_vnc AlwaysShared=1 AcceptPointerEvents=0 AcceptKeyEvents=0 AcceptCutText=0}
      set exe_kill {$::rep/bin/kill.exe}
      set rep_tmp $env(temp)
   }

   {Linux} {
      # config Linux
      set exe_vncviewer {vncviewer $::don($s,ip):$::port_vnc}
      set exe_demo {x11vnc -display :0 -shared -viewonly -forever -rfbport $::port_vnc -allow $l_ip}
      set exe_kill kill
      set rep_tmp /tmp
   }

   {default} {
      # config autres Unix ?
      set exe_vncviewer vncviewer
      set exe_demo {x11vnc -display :0 -shared -viewonly -forever -rfbport $::port_vnc -allow $l_ip}
      set exe_kill kill
      set rep_tmp /tmp
   }
  }
```

Protocole utilisé par Tkontrole

Version du protocole décrite : 1.1

Tous les transferts sur le socket se font avec fin de ligne en cr+lf.

Description du protocole de connexion au serveur

1) Quand la connexion est établie, il y a contrôle par le serveur de l'ip du client, avec rejet éventuel si l'adresse n'est pas dans la liste "ip_accept". Dans ce cas, le serveur ferme le socket après avoir envoyé le mot "refus" au client.
Si le serveur est configuré avec un mot de passe non vide (écrit dans le fichier *pass* du dossier de Tkontrole-serveur), alors le serveur envoie au client une clef de cryptage de 2 caractères. Le client doit alors crypter le mot de passe 2 fois, en utilisant la clef « ts » puis la clef envoyée par le serveur à l'aide du cryptage DES, puis renvoyer le mot de passe au serveur qui valide ou non la connexion.
Si la connexion est refusée, le serveur ferme le socket après avoir envoyé le mot "refus" au client.
Dans tous les cas, si la connexion est acceptée, le mot "ok" est envoyé et la connexion se poursuit.

2) Attente par le serveur du nom de l'utilisateur connecté sur le client.

3) Le serveur se met alors en écoute du client sur le socket attribué. Il redonnait les commandes suivantes :

capture :
Provoque l'envoi au client d'une capture d'écran.
Le serveur envoie dans un premier temps la taille de la capture en octets, puis le fichier est envoyé en mode binaire. L'image transmise est au format « gif ».

blocage+ :
Le serveur provoque l'affichage en premier plan d'une image « écran bloqué ». le blocage d'écran reste actif tant qu'il n'est pas annulé par la commande blocage- ou que le dernier client est déconnecté.

blocage- :
Cette commande provoque la destruction de l'image « écran bloqué ».

message :
Envoi d'un message du client vers le serveur.
Le client envoie le message sous forme d'un fichier texte. La taille du fichier est envoyée en premier lieu, puis le fichier lui-même.

version :
Le serveur renvoie le numéro de version en format texte.

controle+ :
Provoque le démarrage d'un serveur VNC permettant la prise de contrôle de l'ordinateur par le client. Le serveur VNC est démarré sans authentification par mot de passe, mais est uniquement disponible pour l'adresse IP du client qui en fait la demande.

controle- :
A réception de cette commande, le serveur stoppe le serveur VNC qui permet la prise de contrôle.

login :
Cette commande provoque l'envoi du nom de la personne connectée sur le serveur à l'instant de cette requête. Si aucun utilisateur n'est connecté, alors 0 est renvoyé. Cette commande existe toujours mais est désuète à partir de la version 2.0 de Tkontrole, qui récupère le login par la commande *etat*.

arret :
Provoque l'arrêt de l'ordinateur serveur.

redemarrage :
Provoque le redémarrage de l'ordinateur serveur.

deconnexion :
Provoque la déconnexion de l'utilisateur sur l'ordinateur serveur.

blocageroute+ :
Cette commande a pour but de couper l'accès à l'internet sur le poste serveur.

blocageroute- :
cette commande restaure l'accès à l'internet.

etat :
Provoque l'envoi de renseignement sur l'état actuel du serveur. Les informations sont renvoyées sous la forme d'une liste de paire de mots : le premier mot indique le paramètre considéré, le deuxième donne l'état actuel du paramètre.
En version 2.0 de Tkontrole, les paramètre envoyées sont :

blocage_route	>>>>	peut valoir 0 ou 1
controle	>>>>	peut valoir 0 ou 1
blocage	>>>>	peut valoir 0 ou 1
login	>>>>	même effet que la requête login

demo+ :
Quand le client envoie au serveur cette commande, c'est dans le but de faire une démonstration. Le client démarre un serveur VNC sans authentification par mot de passe, mais uniquement disponible pour les adresses IP des serveur Tkontrole qui sont ciblés par le client Tkontrole. Le serveur Tkontrole, quand il reçoit l'ordre, démarre un client VNC.

demo- :
Provoque l'arrêt du client VNC permettant de suivre la démo envoyée par le client Tkontrole.

fin :
Le client annonce qu'il veut stopper la connexion. Provoque la fermeture du socket concerné sur le serveur. Cette commande permet de clore correctement une connexion, notamment d'annuler le blocage du serveur si plus aucun client ne reste connecté.